R E M A R K S

Claims 1, 3-5, 7-11, and 13 were presented for examination and were rejected. The applicants respectfully request reconsideration in light of the amendments and the following comments.

Claims 1, 3, 4, 7, 9, and 10 have been amended.

Support for the amendment to claims 1 and 9 can be found at paragraph [0047] and elsewhere the Specification.

Support for the amendment to claims 3 and 10 can be found at paragraph [0054] and elsewhere in the Specification.

Support for the amendment to claim 4 can be found at Figure 7 and paragraph [0038] and elsewhere in the Specification.

35 U.S.C. § 101 Rejection of Claims 1, 3-5, 7 and 8

Claims 1, 3-5, 7 and 8 were rejected under 35. U.S.C. 101 for failing to recite statutory subject matter. The claims have been amended recite that their tasks are performed by a server and/or a telecommunications device. In their amended form, the claims are tied to a particular machine. For this reason, the applicants respectfully submit that the rejection is overcome.

35 U.S.C. § 103 Rejection of Claims 1, 3, 5, 8, 9 and 11

Claims 1, 3, 5, 8, 9, and 11 were rejected under 35 U.S.C. § 103 as being unpatentable over G. Freund, U.S. Publication 2003/0167405 (hereinafter "Freund") in view of K. Hoene, U.S. Publication 2002/0199116 (hereinafter "Hoene"). The applicants respectfully traverse.

Claim 1, as amended, recites:

> 1. A method comprising:
>
> detecting, at a server, that a device is attempting to connect to a network;
>
> receiving, at the server, a token from the device, wherein the token is in one of:
>
> i. a first state in which the content of the token indicates that the token has not been modified by the device, and
>
> ii. a second state in which the content of the token indicates that the token has been modified by the device, wherein when the token is in the second state, the content of the token comprises:
>
> – an indication that the execution of a security software executing on the device was suspended, and
>
> **– an identification of a network to which the device was connected when the execution of the security software was suspended;**
>
> when the token is in the second state, determining, at the server, if the device was previously connected to an untrusted network; and
>
> if the device was connected to an untrusted network, evaluating the integrity of data on the device, wherein the integrity evaluation is performed by at least one of the device and the server.
>
> (*emphasis supplied*)

Neither Freund nor Hoene teach or suggest, alone or in combination, what claim 1 recites — namely, receiving a token which, when in the second state, includes an identification of the network to which a device was connected when the execution of security software was suspended.

The present invention detects devices that can pose a security threats to the networks to which they connect. For example, in accordance with claim 1, when an anti-virus program is turned off on a computer, the content of a token residing on the computer is changed. In particular, the content is changed to indicate two things: (1) that the anti-virus program was turned off and (2) an identification of the network to which the computer was connected at the time when the anti-virus program was turned off.

At a later time, when the computer attempts to connect to another network, the content of the token is examined to determine if the anti-virus program has been turned off while the computer has been connected to a network of questionable security. When this is

the case, an integrity check is performed on the data residing on the computer to ensure that the computer is not infected with a virus.

The reason for examining the token is that when the execution of anti-virus software on a device is suspended, this device is predisposed to become infected with viruses. The present invention recognizes devices that have such predisposition and performs integrity checks on data located on such devices.

Claim 4, prior to this amendment, recited the use of tokens. In rejecting claim 4, the Office conceded that Freund and Hoene do not teach determining whether a token has been altered. (*See* page 5 of the pending Office Action) The Office, however, advanced T. Noguchi, U.S. Publication 2003/0005333 (hereinafter "Noguchi") as teaching the detection of whether a token has been altered.

The applicants agree that Noguchi contains a discussion of detecting whether a token has been altered. However, Noguchi fails to teach the use of tokens that indicate when the execution of security software on a device has been suspended. In particular, Noguchi fails to teach receiving a token which, when in the second state, includes an identification of the network to which a device was connected when the execution of security software was suspended.

For these reasons, the applicants respectfully submit that the rejection of claim 1 is overcome.

Because claims 3, 5, and 8 depend on claim 1, the applicants respectfully submit that the rejection of them is also overcome.

Claim 9, as amended, recites:

> 9. An apparatus comprising:
>
> a memory; and
>
> a processor, coupled to the memory, for:
>
> detecting that a device is attempting to connect to a network;
>
> receiving a token from the device, wherein the token is in one of:
>
> i. a first state in which the content of the token indicates that the token has not been modified by the device, and
>
> ii. a second state in which the content of the token indicates that the token has been modified by the device, wherein when the token is in the second state, the content of the token comprises:
>
> – an indication that the execution of a security software executing on the device was suspended, and
>
> **– an identification of a network to which the device was connected when the security software was suspended;**
>
> when the received token is in the second state, determining if the device was previously connected to an untrusted network; and
>
> if the device was connected to an untrusted network, evaluating the integrity of data on the device.
>
> (*emphasis supplied*)

For the same reasons as for claim 1, the applicants respectfully submit that the rejection of claim 9 is overcome.

Because claim 11 depends on claim 9, its rejection is also overcome.

35 U.S.C. § 103 Rejection of Claims 4 and 10

Claims 4 and 10 were rejected under 35 U.S.C. § 103 as being unpatentable over G. Freund, U.S. Publication 2003/0167405 (hereinafter "Freund") in view of K. Hoene, U.S. Publication 2002/0199116 (hereinafter "Hoene") and further in view of T. Noguchi, U.S. Publication 2003/0005333 (hereinafter "Noguchi").

Because claims 4 and 10 depend on claims 1 and 9, respectively, and because Noguchi fails to cure the deficiencies of Freund and Hoene, the applicants respectfully submit that their rejection is overcome.

35 U.S.C. § 103 Rejection of Claims 7 and 13

Claims 7 and 13 were rejected under 35 U.S.C. § 103 as being unpatentable over G. Freund, U.S. Publication 2003/0167405 (hereinafter "Freund") in view of K. Hoene, U.S. Publication 2002/0199116 (hereinafter "Hoene") and further in view of Daenen, U.S. Publication 2003/0140151 (hereinafter "Daenen").

Because claims 7 and 13 depend on claims 1 and 9, respectively, and because Daenen fails to cure the deficiencies of Freund and Hoene, the applicants respectfully submit that the rejection of them is overcome.

Request for Reconsideration Pursuant to 37 C.F.R. 1.111

Having responded to each and every ground for objection and rejection in the last Office action, applicants respectfully request reconsideration of the instant application pursuant to 37 CFR 1.111 and request that the Examiner allow all of the pending claims and pass the application to issue.

If there are remaining issues, the applicants respectfully request that Examiner telephone the applicants' attorney so that those issues can be resolved as quickly as possible.

Respectfully,
Martin Kappes et al.

By **/Kiril Dimov/**
Kiril Dimov
Reg. No. 60490
732-578-0103 x215

DeMont & Breyer, L.L.C.
Suite 250
100 Commons Way
Holmdel, NJ 07733
United States of America